

Remarks

The amendments to claim 1 and 3

Examiner will immediately see that the amendments to these claims do not affect their scopes. Both claims have been amended to eliminate the occurrence of the word “may”
 5 and claim 3 has been made dependent from claim 1.

The traversal of the rejections

The traversal of the rejections based on “Software Watermarking” and Moskowitz

In the *Submission* that accompanied the RCE, Applicants argued that Software
 10 Watermarking not only did not disclose or imply the use of watermarks to *authenticate*
 software, i.e., to ensure that the code has not been altered since it was watermarked (cf.
 Specification, page 6 lines 5-12), as opposed to the use of watermarks to embed a
 message such as a copyright notice or customer identification number in the software, but
 actually taught away from the use of watermarks for authentication:

15 What Collberg, *Software watermarking* is chiefly concerned with is the
 difficulty of watermarking something which is as malleable as executable
 code. For example, static watermarks in executable code can be removed
 simply by obfuscating the executable code until the watermark is no
 longer detectable (see Section 2.3). For that reason, Collberg, *Software*
 20 *watermarking* prefers dynamic watermarking, but even there, obfuscation
 can render most dynamic watermarks undetectable (see Section 5.) In
 Section 5, Collberg, *Software watermarking* discloses a new watermarking
 technique called “dynamic graph watermarking” which has more
 resistance to obfuscation attacks. The conclusion which must be drawn
 25 from Collberg, *Software watermarking* is that only the most complex
 dynamic watermarking techniques are of any use in protecting executable
 code.

Watermarking and authentication

30 While Collberg’s pessimism about watermarking executable code may be
 justified when the watermark is used to show ownership, Applicants have
 demonstrated that even simple static watermarking is an effective way to
authenticate executable code. The reason that this is so is that in
 authentication, loss or corruption of the watermark is *proof that the code*
 35 *has changed since it was watermarked*. Thus, the very property of
 watermarked code that renders the watermark almost useless for showing
 ownership of the code makes the watermark extremely useful for detecting
 faulty transmission of the code or tampering with the code and therefore
 for authenticating the code. (*Submission*, p. 10, line 26 – p. 11, line 17)

Examiner attempts to find disclosures in Collberg of the use of watermarks for authentication of the code, but the cited locations disclose the contrary. For example, the location cited as the right-hand column of page 314 discloses that watermarks made by static transformations of code or data are hard to tamperproof because programs written in languages such as Java cannot observe their own code, while programs that can are highly unusual and of course necessarily disclose that the watermark is in the location being examined. The location cited as the right hand column of page 317 discloses further that static watermarks are susceptible to attacks that increase the static size of the code. Both locations demonstrate again that Software Watermarking is concerned only with retaining watermarks that contain readable messages in the software and has no notion that the lack of a watermark or the alteration of a watermark can *by itself* show that the watermarked code has changed since it was watermarked and is therefore not authentic.

Examiner himself admits that “Collberg does not provide very clear teachings [of the use of watermarks to authenticate programs]” (Office action, p. 5, line 11) and for that reason also cites Moskowitz for these teachings. Moskowitz, however, adds nothing to Collberg concerning the use of watermarks to authenticate software. To begin with, Moskowitz is not concerned with watermarking software at all, but rather with watermarking media content with licensing and ownership information. See col. 1, lines 9-37. The purpose of the watermark in the media content is to make it possible to determine ownership of the media content. Indeed, because media content is not executable programs, there is none of the concern for malicious programs that drives Applicants’ use of watermarks to authenticate executable instructions.

In Moskowitz, the watermark is examined to determine one or the other of the following:

- whether the content has a watermark. If the content does not have a watermark, it is presumed to be pirated.
- whether watermarked content is being used in an unauthorized fashion.

Thus, as described at col. 1, lines 63-66, the watermarks can be used to determine whether a data stream that is expected to contain watermarked material does in fact contain it and/or whether the watermarks contain the expected information. As described at col. 1, lines 66-col. 2, line 5, watermarks can be used to make the same determinations with regard to archived material, and as described at col. 3, lines 1-5, individuals can use watermarks in the same fashion.

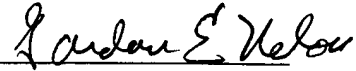
None of this has anything at all to do with Applicants' claimed use of watermarks to determine whether a sequence of code is authentic. Indeed, the word "authentic" and its derivatives appears only four times in Moskowitz (col. 2, lines 21-24; col. 3, lines 1-5; col. 7, lines 10-15, and col. 9, lines 43-46), and in all cases, what is being authenticated is not the media content, but rather the contents of the watermark. Because Moskowitz adds nothing to Software Watermarking regarding authentication of executable code, the combination of Moskowitz and Software Watermarking does not disclose all of the limitations of Applicants' claim 1 as required to establish a *prima facie* case of obviousness. That being the case, claim 1 is patentable over the references. As Examiner will easily see, independent claims 18 and 21 are patentable over Moskowitz and Software Watermarking as well, as are all of the claims dependent from claims 18 and 21. Further, because dependent claims 6- 7 and 15-17 add further limitations to the process of authentication set forth in claims 1 and 18 respectively, these claims are patentable in their own rights over the references.

Conclusion

Applicants have amended claims 1 and 3 to overcome Examiner's objections thereto and have traversed the rejections of claims 1-28 under 35 U.S.C. 103 as obvious over the Moskowitz and Software Watermarking references. Applicants have therefore met the requirements of 37 C.F.R. 111(b) and respectfully request that Examiner continue the examination and allow the claims as presently amended, as provided by 37 C.F.R. 1.111(a). No fees are believed to be required for this amendment; should any be, please

charge them to deposit account number 501315.

Respectfully submitted,



Attorney of record,
Gordon E. Nelson
57 Central St., P.O. Box 782
Rowley, MA, 01969,
Registration number 30,093
Voice: (978) 948-7632
Fax: (866)-723-0359
12/22/2005

Date

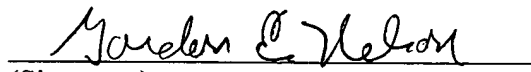
Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on 12/22/2005
(Date)

Gordon E. Nelson, #30,093


(Signature)